United States Department of Homeland Security

Joint Information Bulletin

(U) Look Before You Click: Trojan Horses And Other Attempts To Compromise Networks

21 December 2005

(U) ATTENTION: Federal Departments and Agencies, State Homeland Security Advisors, Security Managers, State and Local Law Enforcement, International Partners, and Information Sharing and Analysis Centers.

(U) DISTRIBUTION NOTICE: Secondary release, dissemination, or sharing of this product is authorized.

(U) This is a Joint Information Bulletin produced by DHS and the Department of State Bureau of Diplomatic Security, Office of Computer Security.

(U) KEY FINDINGS

(U) According to industry security experts, ***the biggest security vulnerability facing computer users and networks is email with concealed Trojan Horse software***—destructive programs that masquerade as benign applications and embedded links to ostensibly innocent websites that download malicious code. ***While firewall architecture blocks direct attacks, email provides a vulnerable route into an organization's internal network through which attackers can destroy or steal information.***

- **(U)** Attackers try to circumvent technical blocks to the installation of malicious code by using social engineering—getting computer users to unwittingly take actions that allow the code to be installed and organization data to be compromised.

- **(U)** The techniques attackers use to install Trojan Horse programs through email are widely available, and include forging sender identification, using deceptive subject lines, and embedding malicious code in email attachments.

- **(U)** Developments in thumb-sized portable storage devices and the emergence of sophisticated keystroke logging software and devices make it easy for attackers to discover and steal massive amounts of information surreptitiously.

(U) ***Security experts believe the most important line of defense in computer security is the user***. User training and awareness about social engineering attack techniques and safe web-browsing practices are integral to a sound computer security posture.

(U) Trojan Horse Software Enables Industrial Espionage

(U) ***An 18-month Israeli police investigation revealed in May 2005 widescale industrial espionage -- Trojan Horse programs had been installed on computers of some of the country's top companies***. In one case, a targeted company employee received an email containing what appeared to be a legitimate business proposal from a reputable company. On opening the proposal, hidden software surreptitiously installed a keylogger -- which captures and stores all keystrokes a user makes -- on the targeted computer.

- **(U)** ***The software also may have propagated the keylogger program throughout the company's network***. At some point, the keylogger executed a program to send files from the company's network to servers in Israel, Germany, and the United States for storage and later transfer to other sites.

(U) Soon after open source reporting of Israeli hacking incidents, government organizations that deal with critical infrastructure protection in Australia, Canada, and the United Kingdom (UK) issued reports that "Trojanized" emails had targeted government and private sector systems and possibly exfiltrated sensitive data since at least November 2003.

- **(U)** ***In the UK***, the National Infrastructure Security Coordination Center (NISCC), part of MI5, noted that ***300 companies have been targeted by Trojan programs delivered by hackers as email attachments, CDs, or links to phony websites***. The NISCC warned that ***the emails used social engineering techniques*** to entice opening the Trojan Horse-infected documents.[1]

(U) Similarities in Attack Methods and Tools

(U) ***The capabilities, tools, and methods that hackers used in these incidents are widely available and can be launched from any access point on the Internet.*** User awareness of hacker tactics is critical to stopping these types of attacks.

(U) Keylogging Threat Grows

(U) According to industry publications, such as Websense 2005 Security Trends Report, ***keylogging software programs are possibly one of the greatest threats lurking on the Internet.*** A keylogger is surveillance hardware or software designed to capture and store in a hidden file every keystroke a user makes. Some keyloggers have the capability to send the file of captured data to any specified receiver without the victim's knowledge. ***New keylogging programs are being developed and posted on websites at an alarming rate***, according to industry reports.

[1] (U) The Wall Street Journal, "Asian Hackers Blamed for Attacks on UK, U.S. Computer Networks," 20 June 2005.

(U) Social Engineering Makes Attacks Easier

(U) ***Recent Trojan Horse attacks have been similar in using social engineering methods, rather than complex technical means, to enter the targeted computer network.*** Social engineering exploits the weakest link in computer network defense—the user—by persuading or deceiving the user, through trust or intimidation, to act out of character.

(U) The social engineer begins by collecting readily available information about the user or organization. The hacker then uses the information to create a plausible story or scenario that causes the victim to take action that releases malicious code into a computer or computer network by clicking on an email link, opening an attachment, or downloading from portable media. In many instances, a well-crafted email that appears to be a legitimate communication gives the recipient a false sense of security regarding the content or attachments.

- **(U)** ***A significant social engineering trend has emerged over the past year -- targeting Trojanized email inquiries, called "spearphishing,"to selected business users.*** The email often claims to be from a recipient's colleague or company's human resources or help desk department. It refers to familiar information to gain the user's trust and encourage clicking the icon, which installs infected software.[2,3,4] Previously, hackers more commonly used mass emailings to thousands of potential targets, hoping that one or more would take the bait and unwittingly install malicious software (a technique called "phishing").

(U) GAO Report Highlights Attacks

(U) A May 2005 Government Accountability Office (GAO) report listed examples of malicious email attacks against U.S. government organizations. In one example, an email claiming to be from an Immigrations and Customs Enforcement (ICE) agent referred users to a bogus website to attempt to steal money from relatives of U.S. soldiers killed in Iraq. In a separate incident, users received spoofed FBI emails containing a link to a fraudulent website that solicited verification of personal information to avoid further investigation. The FBI has issued a public statement alerting the public to the recent email scheme. Similar incidents involved spoofed emails from the Federal Deposit Insurance Corporation and the Internal Revenue Service that tricked recipients into accessing official-looking websites and disclosing personal and financial data. An email sent to State Department employees attempted to dupe them into clicking on a purported State Department link, which then sent the user to a fraudulent website that downloaded malicious code. For more information on how to defend yourself from spoofed emails and phishing attacks, visit the US CERT and the CERT Coordination Center webpages at http://www.cert.org/tech_tips/email_spoofing.html and http://www.us-cert.gov/cas/tips/ST04-014.html

—US Government Accountability Office, GAO-05-231, "Report to Congressional Requesters, Information Security, Emerging Cybersecurity Issues Threaten Federal Information Systems," May 2005, Table 2, page 43.

[2] (U) Australian Government Department of Defense, "DSD Advisory DA-2005-01 Computer Security Advisory From The Information Security Group – Defense Signals Directorate," 16 June 2005, http://www.dsd.gov.au/_lib/pdf_doc/advisories/DA-2005-01.pdf.

[3] (U) Public Safety and Emergency Preparedness Canada, "Information Note Number: IN05-001 Targeted Trojan Email Attacks," 16 June 2005, http://www.ocipep.gc.ca/opsprods/info_notes/IN05-001_e.asp#top.

[4] (U) UK National Infrastructure Security Co-ordination Centre (NISCC), "NISCC Briefing 08/2005 Issued 16 June 2005 – Targeted Trojan email Attacks," http://www.uniras.gov.uk/niscc/docs/ttea.pdf.

(U) NEW DEVELOPMENTS IN HARDWARE DEVICES AID HACKERS

(U) ***Hackers rely on hardware to install their espionage tools.*** As with email-based attacks, social engineering plays a large role in getting the victim to connect the hardware to his or her computer system.

- **(U)** In the Israeli industrial espionage cases, hackers sometimes used a floppy disk to inject malicious code into a computer. The floppy disk was sent through the postal service to a specific individual at a targeted company.

(U) ***Hackers, however, have been quick to adapt to the computer industry's move away from floppy disks and toward cheap, high-capacity portable storage devices such as Universal Serial Bus (USB) drives*** (some nicknamed "thumb drives" because they are about the size of a thumb).

(U) USB Drives: Pernicious Tools for Insiders?

(U) The latest USB drives have a storage capacity of 2 gigabytes, compared to a standard 1.44 megabyte floppy disk. The majority of new computers on the market today come with at least two ports, active by default, into which a USB drive can be quickly and easily inserted. Once plugged in, a USB drive appears to the operating system as just another peripheral hard drive, allowing easy transfer of the computer's data to the USB device or malicious programs from the device onto the computer.

Examples of USB Drives

Figure 1: Unclassified

(U) ***A new and pernicious means of gaining unauthorized access to a network is the use of a USB keylogger.*** The device combines the storage and physical size of a USB drive with keylogging software. These keyloggers connect in-line between a computer's keyboard and processing unit, if the computer has a USB keyboard. If the computer does not have a USB keyboard, there are keyloggers that fit in-line for the standard Personal System 2 keyboard as well. The device captures and stores all of the user's keystrokes without being detected by the computer's operating system. The small device blends in with other connections behind the computer, minimizing the chances of casual discovery. One USB keylogger is advertised as having the capability to store over two million keystrokes, which, according to the manufacturer, is over one year's worth of typing, or about 300,000 words.

(U) Because these portable USB storage devices require physical access to the victim's computer, hackers use social engineering to get them installed. For example, attendees at a recent computer security conference proposed that malicious USB devices could be installed by:

- **(U)** Paying janitorial or other routine service personnel to plug the devices in while doing their otherwise innocuous work.

- **(U)** Using malicious USB devices as advertising giveaways in the expectation that employees would take and use such trinkets.

(U) Source: The US-CERT Technical Cyber Security Alert TA05-189A, titled "Targeted Trojan Email Attack," 08 July 2005, http://www.us-cert.gov/cas/techalerts/TA05-189A.html.

(U) Black Hat 2005 "Plug and Root" Briefing

(U) *At the Black Hat 2005 computer security conference, security researchers described how the "autorun" feature of an Operating System, such as Windows XP, could be tricked into interpreting an attached USB device as non-removable media, such as an internal hard drive. The USB device then could operate as a hardware Trojan, able to run malicious code loaded on the device by the perpetrators.*

(U) *"Plug and Root," The USB Keys to the Kingdom, 27 July 2005*

(U) *http://www.blackhat.com/presentations/bh-usa-05/BH_US_05-Barrall-Dewey.pdf*

Figure 2: Unclassified

(U) SUGGESTED PROTECTIVE MEASURES

(U) Computer users can take steps to defend themselves against these sorts of attacks. Many defenses are technical, but others focus on improving user training and awareness.

(U) Technical Measures

- **(U)** ***Attachments:*** Perform a thorough review of operational needs to determine the types of required attachments. Implement a default deny rule, allowing only those attachment types with a verifiable business need and associated approved software. Block all other attachments.

- **(U)** ***Spoofed Email:*** Block email that does not originate from an internal email server and claims to be from the "same domain" (same .gov, .com, .mil, .org, etc) email address.

(U) ***HTML Delivery:*** Most reported compromises are the result of users not abiding by or following basic computer security practices, particularly when using email. Outright rejection of HTML email likely would present a significant obstacle to many legitimate communications, but HTML can be converted into text or an attachment, thereby neutralizing malicious code. All scripting, redirection attempts, and known exploits should be automatically removed.[5]

(U) User Awareness Measures

(U) An integrated user awareness program combined with technical measures can alleviate a large number of computer security events occurring on networks. Users should be wary of emails with any of the following characteristics:

[5] (U) Ibid.

- **(U)** Email messages written as if they are part of an ongoing conversation, but the user was never part of the original thread.

- **(U)** Email messages disseminated by people or organizations with whom the user never has had contact or that entice the user to click on a link or open an attachment for more information.

- **(U)** Emails with attachments the user was not expecting. This can be any type of attachment, including files with common extensions, such as ".doc" for Microsoft Word files, ".jpg" for photo files, and ".wmv" for video files.

- **(U)** Emails that claim to originate from someone familiar to the user, but the "From" displays differently than in previous messages, such as with a misspelled name or only an email address instead of the sender's name.

- **(U)** Email messages crafted to display the entire body as one big hyperlink, so that if you click anywhere in the body, it will try to open a Web page or download an item.

- **(U)** Email messages that do not display the recipient in either the "To:" or "cc:" fields, or have unfamiliar people in the "To:" field.[6]

(U) REPORTING NOTICE:

(U) DHS and the Department of State encourage recipients of this document to report information related to cyber incidents or vulnerabilities to the US-CERT at webpage: www.us-cert.gov, email: soc@us-cert.gov, or telephone: 1-888-282-0870 (24-hour hotline). DHS and Department of State also encourage recipients to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force (JTTF)—the FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm—and the Homeland Security Operations Center (HSOC). The HSOC can be reached via telephone at 202-282-8101 or by email at HSCenter@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the HSOC. The NICC can be reached via telephone at 202-282-9201 or via email at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact (POC).

(U) For comments or questions related to the content or dissemination of this document, please contact DHS/I&A-PM at IA.PM@dhs.gov.

(U) Tracked by:

(U) CYBR-010200-01-05
(U) CYBR-010300-01-05
(U) CYBR-020200-01-05

[6](U) Ibid.

(U) APPENDIX A

(U) TOOLS OF THE TRADE

(U) Spoofing to Deceive the Victim

(U) Spoofing, or falsifying sender information, is a simple and effective means of tricking a recipient into opening a malicious email. The sender crafts the "From" line to appear as if it is from a known or legitimate sender or from an agency's or corporation's internal address, increasing the likelihood that the recipient will open the message and attachments.

(U) Enticing Subject Line of Email Message

(U) In some cases the "Subject" line of an email or name of an attachment is written to entice the recipient to open it or to click on an internal link. Some enticing subject lines reported in recent industrial espionage incidents include: "Nuclear Weapons Technology Proliferation.doc," "Notepad.exe," "Code Password.doc," or, as in the Israeli episode, some form of business proposal.

(U) Malicious Links in Email or Embedded HTML Code in Attachments

(U) Microsoft Outlook, the most popular email application worldwide, uses Internet Explorer to display email coded in hypertext markup language (HTML). Attackers exploit a known weakness in some earlier versions of Internet Explorer by sending maliciously crafted HTML email messages containing executable code. Users of Outlook's "preview pane" feature do not have to open the email for a vulnerability to be exploited; simply highlighting the message will display it in the preview pane and allow the malicious code to be executed.

(U) Malicious programs also can be placed on a company's or an attacker's web servers and executed when the HTML email is displayed; this means the user's filters, which are designed to block malicious code in the email message itself, are circumvented.

(U) Attackers also can send messages with HTML attachments containing malicious code. When the recipient opens the attachment, the machine may be compromised. These compromises often occur with no indication a program is executing, so the user may be unaware of damage.

(U) Attackers also can take advantage of a reader's curiosity by including deceptively-named links to a malicious website. The user's machine may be compromised when the user clicks on the link and visits the malicious site.

(U) Source: The US-CERT Technical Cyber Security Alert TA05-189A, titled "Targeted Trojan Email Attack," 08 July 2005, http://www.us-cert.gov/cas/techalerts/TA05-189A.html.